PROPOSED CHARGING LETTER

Mr. Ryan Adams

Re: Alleged Violation of the Arms Export Control Act and the International Traffic in Arms Regulations

Dear Mr. Adams:

The Department of State (Department) charges you (Respondent) with a violation of the Arms Export Control Act (AECA) (22 U.S.C. 2751 *et seq.*) and the International Traffic in Arms Regulations (ITAR) (22 C.F.R. Parts 120-130) in connection with the unauthorized provision of defense services to the United Arab Emirates (UAE). A total of one charge is alleged at this time.

The essential facts constituting the alleged violation are described herein. The Department reserves the right to amend this proposed charging letter, including through a revision to incorporate additional charges stemming from the same misconduct of Respondent. Please be advised that this proposed charging letter, pursuant to 22 C.F.R. § 128.3, provides notice of our intent to impose debarment or civil penalties or both in accordance with 22 C.F.R. §§ 127.7 and 127.10.

When determining the charges to pursue in this matter, the Department considered several aggravating factors, including: (a) Respondent did not disclose the violation to the Department; (b) the violation and surrounding circumstances demonstrate Respondent's disregard for the requirements of the ITAR and for Respondent's export compliance responsibilities; and (c) the required license or other approval for some of the conduct at issue would have not been granted by the Department.

The Department also considered a mitigating factor. Respondent entered into agreements with the Directorate of Defense Trade Controls (DDTC) tolling the statutory period that applies to enforcement of the AECA and the ITAR.

This proposed charging letter describes one alleged violation for the period from January 2016 to November 2019.

JURISDICTION

Respondent is a resident of the United States and a U.S. person within the meaning of § 120.15 of the ITAR. Respondent is subject to the jurisdiction of the United States.

During the period covered by the violation set forth herein, Respondent was engaged in the provision of defense services and was not registered with DDTC, in accordance with § 38 of the AECA and § 122.1 of the ITAR. The described violation relates to defense articles described in Category XI(b) and defense services described in Category XI(d) of the United States Munitions List (USML), § 121.1 of the ITAR, at the time the violations occurred.

BACKGROUND

Between January 2016 and November 2019, Respondent was employed by the DarkMatter Group (DarkMatter), a privately held technology and cyber services company headquartered and organized in the UAE that provided cyber services to the UAE government. Prior to working at DarkMatter, a foreign corporation registered in the UAE, Respondent was employed by CyberPoint International LLC (CyberPoint), a U.S.-based company that provided cyber services to the UAE government pursuant to ITAR licenses or other approvals, including technical assistance agreements. CyberPoint and DarkMatter were competitors, and in late 2015 and early 2016, the UAE government transitioned its contracts for cyber services from CyberPoint to DarkMatter. During this time period, DarkMatter hired certain former U.S.-person managers of CyberPoint, including Respondent.

Respondent possessed computer network exploitation (CNE) expertise that included the development, maintenance, deployment, and operation of software and hardware designed to obtain unauthorized access to electronic devices and accounts. Respondent used his CNE expertise to provide and support CNE services that DarkMatter provided for the benefit of the UAE government.

The systems developed, maintained, deployed, and operated by Respondent allowed DarkMatter to gain unauthorized access to, and to thereby acquire data from, computers, electronic devices, and servers around the world, including on computers and servers in the United States, as well as computers and servers that communicated with computers in the United States and were connected to and part of the Internet, in support of the UAE's intelligence gathering efforts. In addition,

at least one of the CNE systems developed and deployed by Respondent was an ITAR-controlled defense article, and Respondent did not obtain the required license or other approval from the Department to provide defense services to foreign persons in connection with such an article.

On September 14, 2021, Respondent, along with two other individuals, entered into a deferred prosecution agreement (DPA) with the U.S. Department of Justice to resolve charges related to his activities with DarkMatter. Respondent acknowledged and agreed to the filing of a two-count Criminal Information charging him with: (1) knowingly and willfully conspiring, in violation of 18 U.S.C. § 371, to violate the AECA and ITAR; and (2) knowingly conspiring, in violation of 18 U.S.C. § 371, to commit access device fraud, and computer fraud and abuse, in violation of 18 U.S.C. §§ 1029 and 1030. Respondent admitted, accepted, and acknowledged under oath that the facts and description of his conduct, as set forth in the Factual Statement attached to the DPA, are true and accurate.

VIOLATIONS

The facts underlying the ITAR violation addressed in this proposed charging letter are derived primarily from the Factual Statement attached to the DPA. The violation involved the unauthorized provision of defense services to DarkMatter and the UAE government.

Unauthorized Provision of Defense Services to the UAE

Between approximately January 2016 and November 2019, Respondent and DarkMatter provided the UAE government with various cyber services, including CNE services and related support activities. Prior to hiring former employees of CyberPoint, DarkMatter did not have sufficient CNE experience or expertise to engage in CNE activity. Accordingly, DarkMatter obtained that CNE expertise, in part, by hiring key U.S. person managers of CyberPoint, including Respondent.

CyberPoint, through its employees and legal counsel, informed Respondent that if Respondent joined DarkMatter, Respondent would need his own TAA or license from DDTC to continue to provide the defense services Respondent had been previously providing to the UAE government under CyberPoint's TAA. Despite this warning and Respondent's awareness that DarkMatter hired him and his former CyberPoint coworkers to provide the same CNE operations and related

services for intelligence purposes to the UAE government, Respondent did not seek or obtain a license or other approval from the Department.

Certain CyberPoint employees, known as the "Raven Team," were former U.S. Intelligence Community employees, and some had active U.S. security clearances or had previously held active security clearances, including Respondent. DarkMatter offered these managers higher compensation packages as compared to the compensation they had received from CyberPoint.

The U.S.-person managers who accepted employment with DarkMatter, including Respondent, became the founding members of a Raven Team successor at DarkMatter, which was referred to as the Cyber Intelligence-Operations (CIO) group. When the CIO group was created, its employees, including Respondent, operated in the same building, with the same terminals, setup, and computer infrastructure from which they operated under CyberPoint.

Starting in or about January 2016, Respondent was Director of Cyber Operations, and he remained in that position until in or about October 2016. As Director of Cyber Operations at DarkMatter, Respondent's duties included briefing the UAE government on the implementation of CNE operations against targets approved by the UAE government, supporting the development and integration of CNE tools, and managing the CIO group's operations. After December 2016, Respondent moved to various different roles supporting the CIO group until October 2017. Respondent was not directly involved with the CNE operations described herein after October 2017. Having migrated out of the CIO operations department entirely in approximately December 2017, Respondent is unaware of CIO operations after that date.

The CIO group was principally dedicated to conducting CNE operations, as well as providing all manner of support for CNE operations, on behalf of and for UAE government agencies. The CNE services conducted by the CIO group provided access to information and data from thousands of targets around the world, and involved the following services: (a) the acquisition, integration, and development of computer exploits from the United States and elsewhere; (b) the acquisition, development, and deployment of customized systems and infrastructure to support CNE activities, including anonymizing software servers, and hardware systems; and (c) collecting exfiltrated data from exploited devices, computers, and servers, and passing such data to the CIO group and UAE government agencies, for further analysis.

Among his other activities, Respondent created certain zero-click computer hacking and intelligence gathering systems that were specially designed, developed, maintained and operated by Respondent to access tens of millions of devices for the UAE government's intelligence purposes. The services performed by Respondent in connection with the relevant systems constituted defense services under USML Category XI(d) because: (a) the relevant systems were electronic systems, equipment, or software that were specially designed for intelligence purposes that collect, survey, monitor, or exploit, or analyze or produce information from the electromagnetic spectrum as described in USML Category XI(b); and (b) Respondent assisted foreign persons in the use, design, development, engineering, production, modification, testing, maintenance, processing, or operation of the relevant systems. Respondent did not have a license or other approval to furnish such ITAR-controlled defense services.

RELEVANT ITAR REQUIREMENTS

The relevant period for the alleged conduct is January 2016 through November 2019. The regulations effective as of the relevant period are described below. Any amendments to the regulations during the relevant period are identified in a footnote.

Part 121 of the ITAR identifies the items that are defense articles, technical data, and defense services pursuant to § 38 of the AECA.

Section 124.1(a) of the ITAR provides that any U.S. person who intends to furnish a defense service must obtain the approval of the DDTC prior to the furnishing of defense services, unless the furnishing qualifies for an exemption under the provisions of the ITAR.

Section 127.1(a)(1) of the ITAR provides that is unlawful to export or attempt to export from the United States, any defense article or technical data, or to furnish any defense service for which a license or written approval is required by the ITAR without first obtaining the required license or written approval from DDTC.

CHARGES

Charge 1: Unauthorized Provision of Defense Services to DarkMatter

Respondent violated 22 C.F.R. § 127.1(a)(1) one time when Respondent provided ITAR-controlled defense services to DarkMatter and the UAE government without a license or other approval from the Department.

ADMINISTRATIVE PROCEEDINGS

Pursuant to 22 C.F.R. § 128.3(a), administrative proceedings against a respondent are instituted by means of a charging letter for the purpose of obtaining an Order imposing civil administrative sanctions. The Order issued may include an appropriate period of debarment, which shall generally be for a period of three (3) years, but in any event will continue until an application for reinstatement is submitted and approved. Civil penalties, not to exceed $1,272,251, per violation of 22 U.S.C. § 2778, may be imposed as well, in accordance with 22 U.S.C. § 2778(e) and 22 C.F.R. § 127.10.

A respondent has certain rights in such proceedings as described in 22 C.F.R. Part 128. This is a proposed charging letter. In the event, however, that the Department serves Respondent with a charging letter, Respondent is advised of the following:

You are required to answer a charging letter within 30 days after service. If you fail to answer the charging letter, your failure to answer will be taken as an admission of the truth of the charges and you may be held in default. You are entitled to an oral hearing, if a written demand for one is filed with the answer, or within seven (7) days after service of the answer. You may, if so desired, be represented by counsel of your choosing.

Additionally, in the event that Respondent is served with a charging letter, Respondent's answer, written demand for oral hearing (if any), and supporting evidence required by 22 C.F.R. § 128.5(b), shall be in duplicate and mailed to the administrative law judge designated by the Department to hear the case at the following address:

USCG, Office of Administrative Law Judges G-CJ,
2100 Second Street, SW, Room 6302
Washington, DC 20593

A copy shall be simultaneously mailed to the Deputy Assistant Secretary for Defense Trade Controls:

Deputy Assistant Secretary Michael Miller
U.S. Department of State
PM/DDTC
SA-1, 12th Floor
2301 E Street, NW
Washington, DC 20522-0112

If Respondent does not demand an oral hearing, Respondent must transmit within seven (7) days after the service of its answer, the original or photocopies of all correspondence, papers, records, affidavits, and other documentary or written evidence having any bearing upon or connection with the matters in issue.

Please be advised also that charging letters may be amended upon reasonable notice. Furthermore, pursuant to 22 C.F.R. § 128.11, cases may be settled through consent agreements, including after service of a proposed charging letter.

The U.S. government is free to pursue civil, administrative, and/or criminal enforcement for AECA and ITAR violations. The Department of State's decision to pursue one type of enforcement action does not preclude it, or any other department or agency, from pursuing another type of enforcement action.

Sincerely,

Michael F. Miller
Deputy Assistant Secretary
Bureau of Political-Military Affairs